Amendments to the Claims:

Please amend the claims as shown. Applicants reserve the right to pursue any cancelled claims at a later date.

1 – 10 (cancelled)

11. (new) A method for granting access to a computer-based object, comprising:

providing a memory card comprising a program code processor;

assigning a public and private key to the memory card;

storing the public and private key assigned to the memory card on the memory card;

providing license information comprising a license code encrypted by the public key assigned to the memory card at a computing device that controls the access to the computer-based object;

generating a symmetric key which is available to the memory card and the computing device from a first random number generated by the memory card and from a second random number provided by the computing device;

transmitting the encrypted license code and a specification of a function to be executed by the memory card for decrypting the encrypted license code which is provided with a hash value encrypted using the symmetric key to the memory card;

decrypting the encrypted hash value by the memory card and checking for agreement with a hash value computed for the specification of the function to be executed by the memory card for decrypting the encrypted license code; and

executing a function for decrypting the encrypted license code by the memory card and transmitting the decrypted license code to the computing device if a result of the check is in agreement,

wherein the decrypted license code provides at least temporary access to the computer-based object.

12. (new) The method as claimed in claim 11,

wherein a public key of a trusted party is provided and protected against manipulations at

the computing device,

wherein the license information is digitally signed by a private key of the trusted party, and

wherein the digital signature of the license information is checked in the computing device with the public key of the trusted party.

13. (new) The method as claimed in claim 11,

wherein the decrypted license code is provided with a hash value encrypted using the symmetric key, and

wherein the encrypted hash value of the decrypted license code is decrypted in the computing device and checked for agreement with a hash value computed for the decrypted license code.

14. (new) The method as claimed in claim 11, wherein the symmetric key is only valid for one access-granting transaction and is regenerated for each new access request.

15. (new) The method as claimed in claim 11,

wherein the license information additionally comprises the public key assigned to the memory card,

wherein the first random number is transmitted, digitally signed by the private key assigned to the memory card, to the computing device,

wherein the digital signature of the first random number is checked in the computing device with the public key assigned to the memory card, and

wherein the second random number is transmitted, encrypted by the public key of the memory card, to the memory card and decrypted there.

16. (new) The method as claimed in claim 11, wherein the encrypted license code and the specification, provided with the hash value encrypted using the symmetric key, of the function to be executed by the memory card for decrypting the encrypted license code are transmitted via a secure communications link from the computing device via a reading device to

the memory card.

17. (new) The method as claimed in claim 11,

wherein a third random number is generated by the memory card and transmitted to the computing device,

wherein a hash value, which is encrypted by the symmetric key and the third random number, is computed by the computing device for the specification of the function to be executed by the memory card for decrypting the encrypted license code and transmitted in encrypted form to the memory card, and

wherein the hash value encrypted by the symmetric key and the third random number is decrypted by the memory card and checked for agreement with a hash value computed for the specification of the function to be executed by the memory card for decrypting the encrypted license code.

18. (new) The method as claimed in claim 17,

wherein a fourth random number is generated in the computing device and transmitted to the memory card,

wherein a hash value, which is encrypted by the symmetric key and the fourth random number, is computed by the memory card for the decrypted license code and transmitted in encrypted form to the computing device, and

wherein the hash value encrypted by the symmetric key and the fourth random number is decrypted in the computing device and checked for agreement with a hash value computed for the decrypted license code.

19. (new) The method as claimed in claim 11, wherein the decrypted license code and a check process sequence are aligned with a respective reference specification for granting the access to the computer-based object.

20 (new) The method as claimed in claim 11, wherein the computer-based object is selected from the group consisting of: operating systems, control or application programs,

services provided by operating systems, functions or procedures, access rights to peripheral devices, and data residing on a storage medium.

21. (new) A control program loaded into a working memory of a computing device and having a code section, comprising:

a code that generates a symmetric key from a first random number generated by a memory card having a program code processor and from a second random number provided by the computing device;

a code that transmits a license code and a specification to the memory card,

wherein the license code is encrypted by a public key assigned to the memory card and, and

wherein the specification, provided with a hash value encrypted using the symmetric key, is of a function to be executed by the memory card for decrypting the encrypted license code;

a code that decrypts the encrypted hash value by the memory card and checks for agreement with a hash value computed for the specification of the function to be executed by the memory card for decrypting the encrypted license code; and

a code that executes a function for decrypting the encrypted license code by the memory card and transmits the decrypted license code to the computing device if a result of the check is in agreement,

wherein the decrypted license code provides at least temporary access to the computer-based object by the computing device.